(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03656 A1

(51) International Patent Classification[7]: H04L 29/12, 12/26, 29/06

(21) International Application Number: PCT/GB01/02939

(22) International Filing Date: 3 July 2001 (03.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0016369.1 3 July 2000 (03.07.2000) GB
0026817.7 2 November 2000 (02.11.2000) GB

(71) Applicant *(for all designated States except US)*: **FIRST GLOBAL COMMUNICATIONS LIMITED** [GB/GB]; Global House, Trostre Industrial Park, Trostre, Llanelli SA14 9UU (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **HERNANDEZ, Jonathan** [GB/GB]; 4 Furnace Terrace, Pontyberem, Llanelli SA1 5AE (GB).

(74) Agents: **BUTLER, Michael, John** et al.; Frank B. Dehn & Co., 179 Queen Victoria Street, London EC4V 4EL (GB).

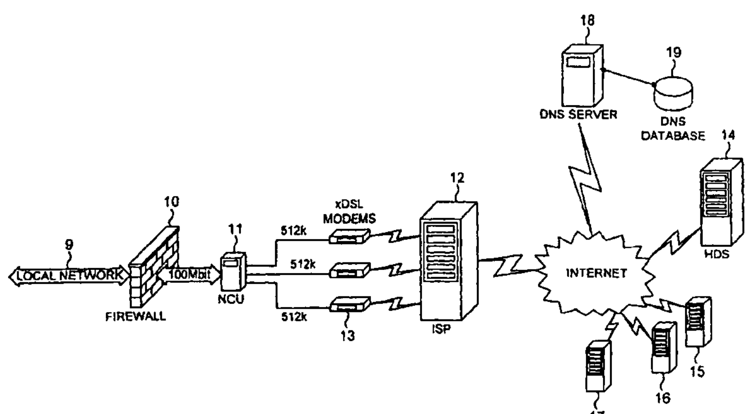
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: MANAGING NETWORK ADDRESSES



(57) **Abstract:** A system for directing network traffic to domains, so as to cope with dynamic network addresses or to provide fault tolerance where a domain has a plurality of available network addresses. The system comprises a domain name server for registering details of a plurality of domains including at least one network address for each domain, means for detecting traffic addressed to domains registered on the domain name server and means for forwarding the traffic for a particular domain to a network address registered on the domain name server in respect of that particular domain. The system further comprises monitoring means which is connected at prescribed intervals to the network addresses registered for the domains and monitors an exchange of data with such network addresses so as to test the validity of the network addresses registered on the domain name server. When a network address is detected by the monitoring means as being invalid it is automatically disabled on the domain name server and network traffic addressed to the domain is automatically directed by the domain name server to a valid network address which is registered on the domain name server as associated with the domain. The valid address may be a new address assigned dynamically which is notified by the domain, or an alternative address already registered.

WO 02/03656 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Managing Network Addresses

The present invention relates to the management of network addresses, and is particularly concerned with the management of IP addresses for servers connected to the Internet which are used, for example to host web sites or e-mail servers.

If a business wishes to host a web site on a server in its own premises and under its control, then it is usually necessary to have a fixed, leased line to an Internet Service Provider (ISP) to provide a sufficiently high speed connection to the Internet and so that a static IP address can be allocated to the web server. Such fixed line connections are relatively expensive.

Higher speeds of connection to the Internet are now becoming possible by the use of relatively inexpensive services such as Asymmetric Digital Subscriber Line ("ADSL") links which can provide e.g. 512 k connections over normal telephone lines. A system such as ADSL provides a connection which is permanently open, and in principle that would make it possible to connect a web server to the Internet via such a route. However, ADSL does not provide subscribers with static IP addresses. Every time that there is an interruption in service, whether for maintenance or through a fault at either end, an IP address will be assigned dynamically. It will therefore be impossible to have a web address which people can use reliably, because the associated IP address will not remain valid. For this reason, it is anticipated that users of ADSL or other systems which involve dynamic IP addressing will have to continue to rely upon web hosting by an ISP as is done currently

with modem or ISDN connections.

For small businesses, there is therefore the choice of having a web site hosted by an ISP or of paying a considerable sum to have a conventional leased line connection. Leased line connections are relatively expensive, and there are certain places, in particular in remote rural areas, where it can be very difficult or even prohibitively expensive to obtain one. On the other hand, using a web site hosted by an ISP has limitations.

A system for dealing with this problem has been proposed by Tzolkin Corporation of Pepperell, MA, USA 01463 and is outlined on the company's web site at www.tzo.com. In the Tzolkin arrangement, a domain name server (DNS) is updated with the IP address from a customer's server. Typically this is achieved by the server transmitting its current IP address at predetermined intervals.

Another problem faced by providers of web sites is the need to balance loads and to provide fault tolerance. US Patent 5,774,660 assigned to Resonate, Inc approaches this problem by having load balancers and backup connections.

Viewed from one aspect the present invention provides a system for directing network traffic to domains, comprising a domain name server for registering details of a plurality of domains including at least one network address for each domain, means for detecting traffic addressed to domains registered on the domain name server and means for forwarding the traffic for a particular domain to a network address registered on the domain name server in respect of that particular domain, the system further comprising monitoring means which is connected at prescribed intervals to the network addresses registered for the domains and monitors an exchange of data with such network addresses so as to test the validity of the network addresses registered on

the domain name server, the system being such that when a network address is detected by the monitoring means as being invalid it is automatically disabled on the domain name server and network traffic addressed to the domain is automatically directed by the domain name server to a valid network address which is registered on the domain name server as associated with the domain.

If a domain is linked to network, i.e. the Internet, through a service provider which allocates a dynamic network address, then this address may change if there is a disconnection between the domain and the service provider. In some arrangements it is even possible for a network address to be altered dynamically whilst there is a connection between the domain and the service provider. To cope with such a problem, in one embodiment of the present invention, the system is arranged to receive details of the current network address from a domain whenever there is a change of network address. The implementation of such a system will require the installation of software at the domain which will preferably detect a change in address immediately and will immediately notify the system of the new address that has been allocated.

With respect to the prior art, a significant difference is the manner in which an invalid network address is detected. The system does not simply wait for software at a domain to advise, at an appropriate time, that there has been a change. Instead the system continually polls the registered addresses by making a connection and exchanging data. By both making a connection and exchanging data the system can detect an invalid address even though in some cases a connection can be made. By detecting an invalid address actively, the system can immediately remove it as a valid address for the domain concerned. If there is an alternative address registered for the domain then this can be used

immediately. If there is not, then the system will have to wait until the domain notifies the system of the newly assigned address. If there is a delay, then there could be a site to which the user seeking access to the domain is directed, with a suitable message of apology for example.

In implementation of the invention, it would be possible for the monitoring means to initiate a connection with a domain at regular intervals, which could for example be a second apart. Alternatively, software at the domain end could be set up to make a connection at intervals and the monitoring means could react if no data is received at the appropriate time. In a preferred system, the monitoring means initiates regular connections, and this is coupled with the domain end reporting any change in network address detected at the domain end.

In the preferred embodiments, notification from a domain of a modified address is virtually instantaneous. This is because in the preferred embodiment software at the domain monitors the address continuously and is made immediately aware of a change in the address, which is forwarded to the system so that the domain name server can be updated. This is distinct from a system in which there is a connection made between the domain and the system at predetermined intervals by means of which the domain transmits its current address to the system so that records are updated on the domain name server. The combination of rapid detection by the system of an invalid address, and rapid advice of a changed address from the domain provides a fast reacting arrangement so that a change can be registered in a matter of a few cycles of it having occurred.

To accommodate such rapid changes, it is important that browsers or the like connecting to a domain do not continually try to use an invalid address that has been

cached by the browser. This can be ensured by setting a very short Time To Live (TTL) parameter on the domain name server (DNS) which is picked up by a browser when attempting to connect to the domain. By setting a low value, such as a second, this ensures that if there is a change in address between one request and another, the new address will always be picked up. The browser will always ask the DNS for an address rather than use a cached value which may be out of date. Such an arrangement is of particular use in another context in which the invention may be used, namely load sharing and / or fault tolerance.

The system above has been described in the context of a domain only having a single network address at any one time so that only a single address is stored by the DNS. When an address is changed, the DNS removes the old address and substitutes the new address. If the monitoring means detects that an address is no longer operational, then the address is removed and a new address is substituted when it is notified to the DNS. However, the DNS can also store more than one address as applicable to a domain. Under such circumstances, if one address becomes invalid then traffic can be switched automatically to another address. Thus if a connection is lost through hardware or communications failure, traffic can be diverted so as to ensure continuous access to the domain. The monitoring means continuously monitors the validity of the IP addresses so that there will be a rapid switch to an alternative address if one address fails.

In such an arrangement, one address may be a primary address and another can be a backup address used only if the primary address fails. For example, the primary address could apply to a connection via a leased line, ADSL or another fast connection whilst the backup address may apply to a slower connection such as ISDN.

Any of the addresses may be allocated dynamically and the system described earlier will apply if there is a change in address.

In such an arrangement, it is also possible to arrange for load balancing. The system could divert traffic to an alternative address if the connection to one address becomes congested, and this may be appropriate if there is a backup address using a slower connection. Alternatively, the system may allocate traffic to the available IP addresses, or at least some of them, continuously. For example, data could be directed to the IP addresses on a "round robin" basis.

In practice, the network will normally be the Internet and the addresses will be IP addresses. The purpose of the domains will normally be to host web sites, although the invention is applicable to other functions. In preferred embodiments of the invention, reference to a "domain" signifies a site where there is a server to which a connection is made. The server may be a dedicated web server, or a server running a number of applications, under a server operating system such as Microsoft Windows NT or Windows 2000 Server (trade marks). However, the expression "server" also extends to a web server environment on a desktop personal computer running suitable software under a desktop operating system such as Microsoft Windows NT Workstation, Windows 2000 Professional, or Windows 98 (trade marks). The site may include several linked servers.

By means of the invention, a small business or home user connected to the Internet via ADSL and an ISP can nevertheless use its own server to host a web site with a suitable domain name. Although the IP address will change in accordance with the dynamic IP address assigned by the ISP, all traffic for the domain name will be intercepted by the DNS and diverted to the currently assigned IP address. Thus people who wish to

visit the web site or connect to the server for any other reason will have no difficulty. Their traffic will be directed to an appropriate IP address.

The DNS which is a part of the system in accordance with the invention provides a "Packet Forwarding Service" which will store the basic IP address allocated when a domain name is allocated. Packets to this address will be intercepted, and will be directed to a currently valid IP address. These functions could be carried out by a single server or by a number of linked servers, and the expression "domain name server" or DNS is intended to cover all such possibilities.

An important requirement of a forwarding service is that it should be resilient. Failure of a server could have consequences for many users. In any event, for upgrade or maintenance purposes it may be desirable to alter the location of a server forming part of the system. In one embodiment the system will issue location data packets - or "heartbeats" - at intervals indicating the IP address to which information should be sent. The domains will detect the location data packets, and in response will transmit their currently assigned IP addresses. Thus, in testing the validity of the address for a domain at regular intervals, the system also advises the domain as to where it should send information about its current IP address. The timing of heartbeat packets could be as desired to ensure continuity, for example being as often as one a second.

In one preferred arrangement, there is provided a Heartbeat Distribution Server ("HDS"), a number of Heartbeat Servers ("HBS") and a Domain Name Server which holds a database including domain names, associated static IP addresses, and any currently assigned dynamic or static IP addresses to which traffic is to be directed. At the user's site is a network control unit ("NCU") which connects to the HDS and obtains the IP

address of an HBS. It establishes a secure connection with the HBS and transmits a unique identifier which is associated with a domain name in the DNS. The currently assigned IP address for the site is transmitted to the HBS which in turn transmits the information to the DNS, where it is stored in the DNS database. Packets which are addressed to the basic IP address assigned to the domain name are diverted to an IP addresses stored in the DNS database.

Once the NCU has registered through an HBS, a heartbeat system is established. The HBS sends a small data packet every second to the address associated with the NCU, and the NCU sends a response back. If the HBS does not receive a response back, then it removes the IP address from its list and informs the DNS which removes it from the DNS database. Meanwhile, the NCU monitors the assigned IP address constantly. As soon as it is altered, the HBS is advised and the new IP address replaces that previously stored. Implementation of this particular aspect is unnecessary if the domain is connected to the Internet with static IP addresses and the system is being used to provide fault tolerance and / or load balancing.

In a preferred arrangement, the NCU operates at a low level to detect a change to an IP address. In one system operating under Microsoft Windows (TM), a Windows API call-back is used to notify the NCU when a change has been detected in the configuration of a network interface such as a card (NIC) or an on board interface. The NCU checks to see if the network address has been altered. If it has, the NCU de-registers the old address and registers the new. This change is notified to the system.

In one preferred implementation, the NCU connects to the Internet through multiple connections, each of which will have its own IP address. This increases the

available bandwidth, and all of the available IP addresses are recorded as associated with the site. Packets addressed to the site are directed to the various IP addresses in rotation to spread load.

In a further enhancement of this system, there may be two connections to the Internet through different ISP's and / or routes, such as satellite and land lines. The system thus has resilience if one ISP or route of communication fails, as the other connection will be available and traffic will automatically be directed to that connection only.

To implement the systems described above, software is required to register static IP addresses associated with remote servers for domains, if desired to transmit heartbeat packets, to record the current IP addresses of the remote servers, and to divert packets addressed to the static IP addresses. Software will also be required for the remote servers of domains, to communicate current IP addresses to the system, either in response to a heartbeat packet from the system or in response to a change detected at the domain.

The invention extends to software for programming data processing means to act in the manner outlined above. Such software may be supplied on physical means such as a CD-ROM or by means of transmission from a remote location, such as over the Internet. The supplied software may be in compressed or encrypted form and may be run on data processing means as an installation routine to install software that can actually be run to implement the invention. The invention also extends to data processing means programmed to operate as described above. There are many aspects of the invention, of which the following are examples.

Viewed from one aspect the invention provides a system for directing network traffic to domains, comprising a domain name server for registering details

of a plurality of domains including at least one domain having a plurality of network addresses, means for detecting traffic addressed to the at least one domain and means for forwarding the traffic for the domain to at least one of the network addresses registered on the domain name server in respect of that particular domain, the system further comprising monitoring means for detecting when one of the network addresses registered in respect of the domain is invalid so that the system automatically directs network traffic addressed to the domain to another, valid network address which is registered on the domain name server as associated with the domain.

Viewed from another aspect the invention provides a system for directing network traffic to domains, comprising a domain name server for registering details of a plurality of domains including at least one network address for each domain, means for detecting traffic addressed to domains registered on the domain name server and means for forwarding the traffic for a particular domain to a network address registered on the domain name server in respect of that particular domain, where at least one domain is connected to the network with a dynamic network address and the domain advises the system when a change in network address is detected at the domain, the changed network address being registered on the domain name server in place of a previous network address registered in respect of the domain, wherein a change in network address is detected at the domain by means of an application program interface call advising of a change of configuration in a network interface.

Viewed from another aspect, the invention provides a system for directing network traffic to domains, comprising a domain name server for registering details of a plurality of domains including at least one network

address for each domain, means for detecting traffic addressed to domains registered on the domain name server and means for forwarding the traffic for a particular domain to a network address registered on the domain name server in respect of that particular domain, where at least one domain is connected to the network with a dynamic network address and the domain advises the system when a change in network address is detected at the domain, the changed network address being registered on the domain name server in place of a previous network address registered in respect of the domain, wherein a change in network address is detected at the domain by means of periodic checks in a routing table.

Viewed from another aspect the invention provides a computer software product for configuring data processing means to provide a system for directing network traffic to domains, the system comprising a domain name server for registering details of a plurality of domains including at least one network address for each domain, means for detecting traffic addressed to domains registered on the domain name server and means for forwarding the traffic for a particular domain to a network address registered on the domain name server in respect of that particular domain, the system further comprising monitoring means which can be connected at prescribed intervals to the network addresses registered for the domains and can monitor an exchange of data with such network addresses so as to test the validity of the network addresses registered on the domain name server, the system being such that when a network address is detected by the monitoring means as being invalid it is automatically disabled on the domain name server and network traffic addressed to the domain is automatically directed by the domain name server to a valid network address which is registered on the domain

name server as associated with the domain.

Viewed from another aspect the invention provides a computer software product for configuring data processing means connectible to a network, so that the data processing means can detect a change in network address and notify a domain name server as to the change in domain, the product configuring the data processing means so that a change in network address is detected by means of an application program interface call advising of a change of configuration in a network interface.

Viewed from another aspect the invention provides a computer software product for configuring data processing means connectible to a network, so that the data processing means can detect a change in network address and notify a domain name server as to the change in domain, the product configuring the data processing means so that a change in network address is detected by means of a change in network address is also detected at the domain by means of periodic checks in a routing table.

Some embodiments of the invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is a schematic overview of a system in accordance with the invention;

Figure 2 is a diagram of an implementation of the invention; and

Figure 3 is a diagram of an alternative implementation of the invention.

Referring to Figure 1, a small business at a site 1 has a server 2 capable of hosting a web site, using an operating system such as Windows NT. This is connected to the Internet via a 512k ADSL connection over telephone line 3 and via an Internet Service Provider (ISP) at a site 4. The business has obtained a domain name from a suitable company such, with an associated

static IP address which may be in the form nnn.n.nnn.nn. The ISP however connects the server 2 to the Internet using a dynamic IP address, so that users wishing to connect to the registered domain will not be able to do so. To resolve the problem, a forwarding service is established by an organisation which is independent of the ISP, at a site 5. This organisation sets up a forwarding server 6 connected permanently to the Internet via a fixed high bandwidth line 7 and a second ISP at a site 8 which provides a static IP address. The server 6 is programmed to provide two services, namely a Connection Information Service ("CIS") and a Packet Forwarding Service ("PFS"). The forwarding server may use an operating system such as Windows NT and may use e.g. a database such as SQL Server to store details of subscribers and the associated IP addresses.

The CIS sends out a heartbeat packet over the Internet at, say, one second intervals on a permanent basis. This heartbeat packet contains details of how to connect to the P'S, i.e the IP address of the server running the P'S. At the remote server 2 of the small business, software has been installed to act as a Heartbeat Packet Receiver ("HPR"). This listens for the heartbeat packets. Once a heartbeat packet has been received, the HPR system connects to the PFS server and registers the current ADSL IP address obtained from the ADSL IP. The PFS server will then divert any traffic addressed to the static IP address to the currently assigned ADSL IP address for the remote server.

In this manner the small business may host its own web site on its own server, whilst avoiding the cost of a leased line, static IP address, connection. Users visiting the web site will not notice that re-direction is taking place.

The forwarding service will normally have a number of subscribers, each of whose remote servers will detect

the heartbeat packets and notify the forwarding server of the currently assigned IP address.

In the arrangement outlined above, the forwarding service accesses the Internet through an ISP. In such an arrangement, the ISP will be notified of the static IP addresses and will transmit traffic addressed to them to the forwarding service. The arrangement as between the ISP and the forwarding service would be the same as if the forwarding address was hosting web sites using the various static IP addresses. If the forwarding service itself had direct access to the Internet, then this arrangement would not be necessary.

Referring now to Figure 2, a local site indicated by network 9 is connected to the Internet through a conventional firewall 10. This has a 100 Mbit connection to a Network Control Unit ("NCU") 11 which is part of the system in accordance with the invention. This is connected to an Internet Service Provider ("ISP") 12 via three 512k xDSL modems 13, which currently would be ADSL modems in the United Kingdom. The ISP is connected to the Internet. The NCU is capable of handling 30Mbits of inbound and outgoing Internet traffic, but in this example is configured to manage 1.5 Mbits. Each ADSL connection is capable of receiving incoming data at up to 512k but of transmitting at 256k only.

Also connected to the Internet is a Heartbeat Distribution Server ("HDS") 14, three Heartbeat Servers ("HBS") 15, 16 and 17, and a Domain Name Server ("DNS") 18 which holds a DNS database 19. A domain name has been allocated to the site 9, with an associated static IP address, and this information is stored in the DNS database.

When the NCU is powered on, it connects to the HDS 14 and requests and receives the IP addresses of two active Heartbeat Servers. The function of the HDS 14 is to manage load balancing and fault tolerance of the

heartbeat servers, of which there may be more than the three indicated in the present example. For example, a heartbeat server may need to be shut down for routine maintenance. All NCU's connected to that HBS would be instructed to remove it from their list and to connect to the HDS for a replacement HBS. If an HBS reaches its maximum NCU connections, then it would remove itself from the HDS list of available HBS's, making itself available again when the load is reduced.

Once the NCU has the IP addresses of two HBS's, it establishes a secure connection with one of them, the other being a backup. The site is identified by a unique combination of the NCU serial number and its Media Access Control (MAC) address. The NCU's serial number is encrypted and is used as a private key, whilst the MAC address is a public key. Using this, the HBS can identify the domain name in the DNS. The NCU has obtained the IP address for each of the connections to the ISP via the three ADSL modems, and transmits these address to the HBS to which it is connected. That in turn transmits the information to the DNS, where it is stored in the DNS database. Packets which are addressed to the static IP address assigned to the domain name are diverted to one of the three IP addresses stored in the DNS database. The DNS is set up to use multiple addresses in rotation, so that network load will be distributed across the connections between the NCU and the ISP.

Using the configuration shown the total bandwidth available for traffic into the site 9 is 1.5 Mbit, but the maximum bandwidth available for a single external user transmitting data to the site 9 is that of a single ADSL connection, currently limited to 512k. However, the NCU is configured so that is can spread the outgoing traffic across all available bandwidth from multiple connections. For each ADSL modem connection the maximum

bandwidth for outgoing traffic is 256k, but by using all three connections the total bandwidth is 768k.

Once the NCU has registered through an HBS, a heartbeat system is established. The HBS sends a small data packet every second to each IP address associated with the NCU, and the NCU sends a response back from each IP address. If the HBS does not receive a response back, then it removes the IP address from its list and informs the DNS which removes it from the DNS database. Meanwhile, the NCU monitors the assigned IP addresses constantly. As soon as one is altered, the HBS is advised and the new IP address replaces that previously stored. The NCU operates at a low level to detect a change to an IP address. Operating under Microsoft Windows (TM), a Windows API (Application Program Interface) call-back is used to notify the NCU when a change has been detected in the configuration of a network interface such as a card (NIC) or an on board interface. The NCU checks to see if the network address has been altered. If it has, the NCU de-registers the old address and registers the new. This change is notified to the system. The NCU also makes periodic checks to see if there is a new or modified gateway entry in the routing table. If the routing table's default gateway entries have change then the NCU registers the modifications and any new IP Addresses with the DNS Server. In both cases the new or modified route (IP Address) is validated prior to registration. To validate a new or modified route the NCU attempts to connect to a known server on the Internet. If the connection is successful then the NCU marks the route as valid and the registration process is initiated. If the route is not valid (the NCU cannot connect to the known server using that route) then the route is marked as a non-Internet route. Non-Internet routes are periodically re-checked in case that route can access the Internet.

If the bad route is re-checked and is able to access the Internet then the route is registered and is noted as being a valid route.

The NCU is capable of managing up to 15 routes and shares the incoming traffic among all registered routes. If a route failure is detected by either the NCU or the Heartbeat server (HBS) then that route is noted as being invalid and is deregistered. The periodic re-check of bad routes will detect when a route becomes active again.

If the NCU detects an interruption in the receipt of heartbeat packets from an HBS, then it can switch to a backup HBS immediately.

In the modified arrangement of Figure 3, the NCU 11 is connected to two different ISP's 20 and 21. The communication to one ISP 20 is via two xDSL modems 22, whereas the other is via a satellite connection 23. This can be used if there is failure of the fixed links. The IP addresses associated with the xDSL connections will be removed from the DNS database, and the IP address associated with the satellite link and ISP 21 will be substituted. Such an arrangement, using two totally different routes to the Internet, will be of use even if static IP addresses are assigned by the ISP's. There will be the options of spreading load over the two routes and of switching between routes if one fails.

Other broad aspects of the systems described which are considered inventive include:

A system for directing data packets over a network to a remote server which is connected to the network by means of a service provider which assigns a dynamic network address, comprising the steps of establishing a static network address to be associated with the remote server, registering the static network address with a forwarding server which is remote from the remote server and the service provider, transmitting from the remote

server to the forwarding server the currently assigned network address associated with the remote server, registering on the forwarding server that currently assigned network address as being associated with the static network address, detecting at the forwarding server data packets addressed to the static network address, and forwarding the detected data packets to the associated currently assigned network address.

Data processing means acting as a forwarding server, comprising means for registering a static network address associated with a subscriber who has a remote server to which a dynamic network address will be assigned, means for receiving from the remote server the currently assigned network address associated with the remote server, means for registering that currently assigned network address as being associated with the static network address associated with the subscriber, detecting at the forwarding server data packets addressed to the static network address, and forwarding the detected data packets to the associated currently assigned network address.

Data processing means for acting as a remote server to which a dynamic network address is assigned, comprising means for detecting the currently assigned network address, and means for transmitting to a forwarding server data which identifies the remote server and the currently assigned network address. Preferably this data processing means comprises means for detecting location data packets indicating the network address of the forwarding server, and means for responding to the location packets by transmitting to the forwarding server the currently assigned network address of the remote server. Again, this aspect of the invention also extends to software for programming data processing means to act as the remote server in the manner outlined above. Such software may be supplied on

physical means such as a CD-ROM or by means of transmission from a remote location, such as over the Internet.

Data processing means acting as a forwarding server, comprising means for registering a principal network address associated with a subscriber who has a remote server which is connected to the network by means of at least two routes with different network addresses, means for registering the network addresses associated with the different routes as being associated with the principal network address, means for detecting data packets addressed to the principal network address, and means forwarding the detected data packets to an active associated network address.

A system for directing data packets over a network to a remote server comprising the steps of establishing a principal network address to be associated with the remote server, registering the principal network address with a forwarding server, registering on the forwarding server at least one currently active network address associated with the remote server, detecting at the forwarding server data packets addressed to the principal network address, forwarding the detected data packets to an active associated network address, and automatically detecting and registering changes in currently active network addresses.

CLAIMS

1. A system for directing network traffic to domains, comprising a domain name server for registering details of a plurality of domains including at least one network address for each domain, means for detecting traffic addressed to domains registered on the domain name server and means for forwarding the traffic for a particular domain to a network address registered on the domain name server in respect of that particular domain, the system further comprising monitoring means which is connected at prescribed intervals to the network addresses registered for the domains and monitors an exchange of data with such network addresses so as to test the validity of the network addresses registered on the domain name server, the system being such that when a network address is detected by the monitoring means as being invalid it is automatically disabled on the domain name server and network traffic addressed to the domain is automatically directed by the domain name server to a valid network address which is registered on the domain name server as associated with the domain.

2. A system as claimed in claim 1, wherein a domain registered on the domain name server is connected to the network with a dynamic network address and the domain advises the system when a change in network address is detected at the domain, the changed network address being registered on the domain name server in place of a previous network address registered in respect of the domain.

3. A system as claimed in claim 2, wherein a change in network address is detected at the domain by means of an application program interface call advising of a change of configuration in a network interface.

4. A system as claimed in claim 2 or 3 wherein a change in network address is detected at the domain by means of periodic checks in a routing table.

5. A system as claimed in claim 2, 3 or 4, wherein prior to a changed network address being notified to the system for registering the network address on the domain name server, the changed network address is validated by attempting a connection to a server on the network.

6. A system as claimed in any preceding claim, wherein a domain has a plurality of connections to the network, and a corresponding plurality of network addresses are registered on the domain name server, and wherein when a network address is detected by the monitoring means as being invalid, network traffic is directed to at least one other of the plurality of registered network addresses.

7. A system as claimed in claim 6, wherein network traffic is shared between valid network addresses for the domain to provide load sharing.

8. A system as claimed in any preceding claim, wherein the monitoring means includes a plurality of heartbeat servers which connect to the domains at periodic intervals, and a heartbeat distribution server which advises domains as to available heartbeat servers to which a connection may be made.

9. A system for directing network traffic to domains, comprising a domain name server for registering details of a plurality of domains including at least one domain having a plurality of network addresses, means for detecting traffic addressed to the at least one domain and means for forwarding the traffic for the domain to

at least one of the network addresses registered on the domain name server in respect of that particular domain, the system further comprising monitoring means for detecting when one of the network addresses registered in respect of the domain is invalid so that the system automatically directs network traffic addressed to the domain to another, valid network address which is registered on the domain name server as associated with the domain.

10. A system as claimed in claim 9, wherein network traffic is shared between valid network addresses for a domain to provide load sharing.

11. A system as claimed in claim 9 or 10, wherein the monitoring means attempts at intervals to make a connection to registered network addresses and detects when a connection is not made.

12. A system as claimed in claim 9 or 10, wherein the monitoring means attempts at intervals to make a connection to registered network addresses and to exchange data, and detects when data exchange is not effected.

13. A system for directing network traffic to domains, comprising a domain name server for registering details of a plurality of domains including at least one network address for each domain, means for detecting traffic addressed to domains registered on the domain name server and means for forwarding the traffic for a particular domain to a network address registered on the domain name server in respect of that particular domain, where at least one domain is connected to the network with a dynamic network address and the domain advises the system when a change in network address is detected

at the domain, the changed network address being registered on the domain name server in place of a previous network address registered in respect of the domain, wherein a change in network address is detected at the domain by means of an application program interface call advising of a change of configuration in a network interface.

14. A system as claimed in claim 13, wherein a change in network address is also detected at the domain by means of periodic checks in a routing table.

15. A system for directing network traffic to domains, comprising a domain name server for registering details of a plurality of domains including at least one network address for each domain, means for detecting traffic addressed to domains registered on the domain name server and means for forwarding the traffic for a particular domain to a network address registered on the domain name server in respect of that particular domain, where at least one domain is connected to the network with a dynamic network address and the domain advises the system when a change in network address is detected at the domain, the changed network address being registered on the domain name server in place of a previous network address registered in respect of the domain, wherein a change in network address is detected at the domain by means of periodic checks in a routing table.

16. A system as claimed in claim 15, wherein a change in network address is also detected at the domain by means of an application program interface call advising of a change of configuration in a network interface.

17. A computer software product for configuring data

processing means to provide a system for directing network traffic to domains, the system comprising a domain name server for registering details of a plurality of domains including at least one network address for each domain, means for detecting traffic addressed to domains registered on the domain name server and means for forwarding the traffic for a particular domain to a network address registered on the domain name server in respect of that particular domain, the system further comprising monitoring means which can be connected at prescribed intervals to the network addresses registered for the domains and can monitor an exchange of data with such network addresses so as to test the validity of the network addresses registered on the domain name server, the system being such that when a network address is detected by the monitoring means as being invalid it is automatically disabled on the domain name server and network traffic addressed to the domain is automatically directed by the domain name server to a valid network address which is registered on the domain name server as associated with the domain.

18. A computer software product for configuring data processing means connectible to a network, so that the data processing means can detect a change in network address and notify a domain name server as to the change in domain, the product configuring the data processing means so that a change in network address is detected by means of an application program interface call advising of a change of configuration in a network interface.

19. A computer software product for configuring data processing means connectible to a network, so that the data processing means can detect a change in network address and notify a domain name server as to the change in domain, the product configuring the data processing

means so that a change in network address is detected by means of a change in network address is also detected at the domain by means of periodic checks in a routing table.

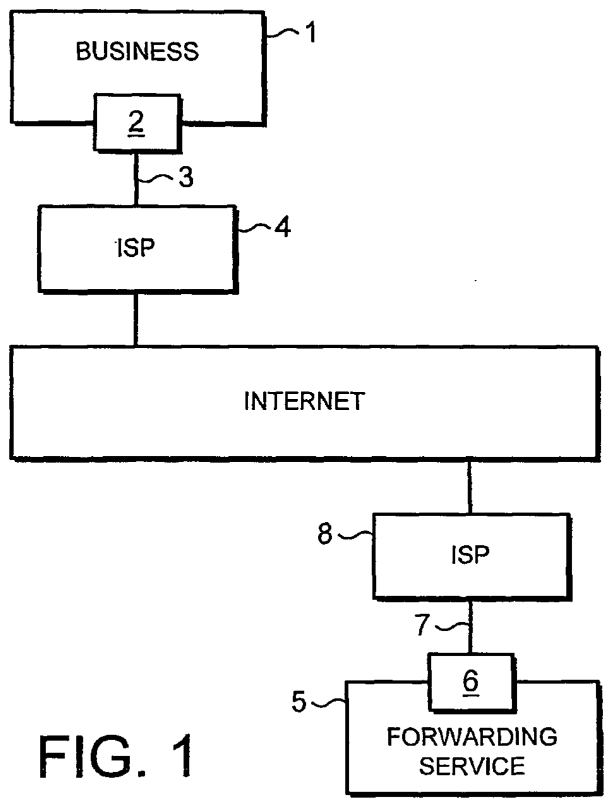


FIG. 1

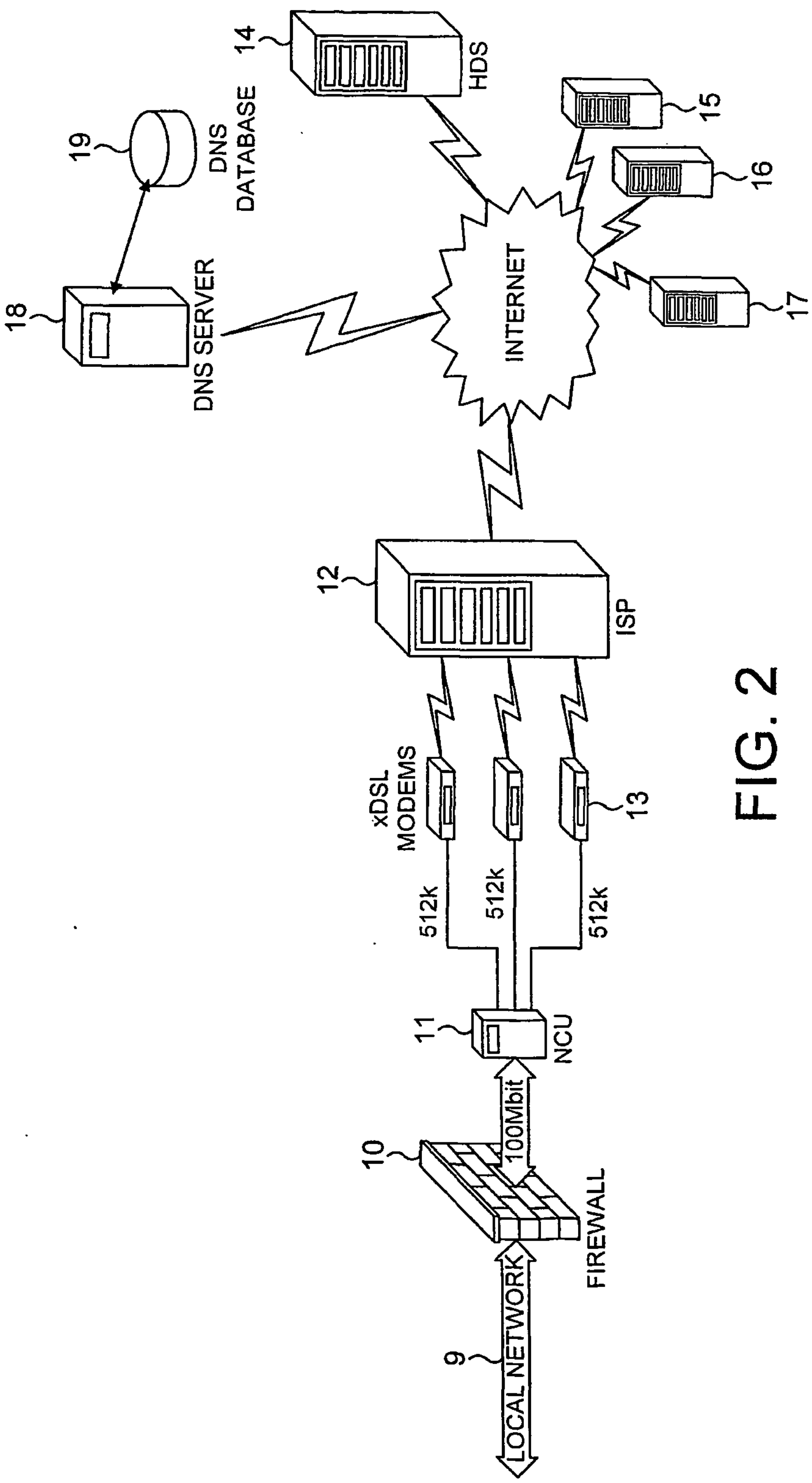

LOCAL NETWORK
9
FIREWALL
10
100Mbit
NCU
11
512k
512k
512k
xDSL
MODEMS
13
ISP
12
INTERNET
DNS SERVER
18
DNS
DATABASE
19
HDS
14
15
16
17

FIG. 2

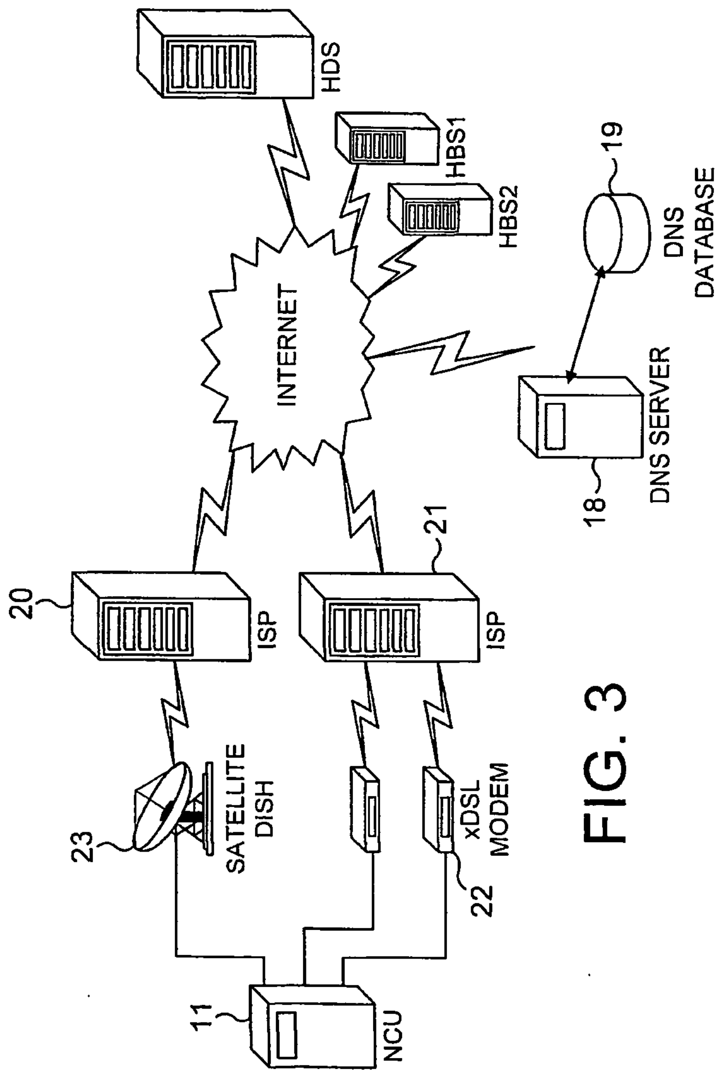

HDS
HBS1
HBS2
INTERNET
19
DNS
DATABASE
18
DNS SERVER
20
ISP
21
ISP
23
SATELLITE
DISH
xDSL
MODEM
22
11
NCU

FIG. 3

INTERNATIONAL SEARCH REPORT

Intei Application No
PCT/GB 01/02939

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/12 H04L12/26 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JAMES FITZGIBBON, TIM STRIKE: "Distributed Computing: Moving from CGI to CORBA" UNISEX 2000 ANNUAL GENERAL CONFERENCE, 'Online! 18 - 23 June 2000, XP002179789 San Diego, California Retrieved from the Internet: <URL:http://www.usenix.org/events/usenix2000/general/full_papers/fitzgibbon/fitzgibbon.pdf> 'retrieved on 2001-10-09!	1-3, 6-12,17
A	pag 7 The service HeartBeat Daemon pag 8 Adding load balancing and redundancy fig. 6	13,15, 18,19

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 October 2001	24/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bertolissi, E

INTERNATIONAL SEARCH REPORT

Interr Application No
PCT/GB 01/02939

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	ALAN ZEICHICK: "TZO Premiere Dynamic DNS Service" ZDNET REVIEWS, 'Online! 12 December 1999 (1999-12-12), XP002179790 Retrieved from the Internet: <URL:http://www.zdnet.com/filters/printerfriendly/0,6061,2409608-79,00.html> 'retrieved on 2001-10-10!	1-3, 6-12,17
A	the whole document	13,15, 18,19
A	TIM HIGGINS: "TZO Dynamic DNS Service" PRATICALLY NETWORKED REVIEWS, 'Online! 22 May 2000 (2000-05-22), XP002179791 Retrieved from the Internet: <URL:http://www.practicallynetworked.com/reviews/tzo.asp> 'retrieved on 2001-10-10! the whole document	1-19
A	A. GULBRANDSEN, P. VIXIE: "RFC 2052 - A DNS RR for specifying the location of services (DNS SRV)" REQUEST FOR COMMENTS, 'Online! October 1996 (1996-10), XP002179792 Retrieved from the Internet: <URL:http://www.alternic.org/rfcs/rfc2000/rfc2052.txt> 'retrieved on 2001-10-10! pag 1 Overview and rationale	1-19
A	FOO S ET AL: "APPROACHES FOR RESOLVING DYNAMIC IP ADDRESSING" INTERNET RESEARCH: ELECTRONIC NETWORKING APPLICATIONS AND POLICY, XX, XX, vol. 7, no. 3, 1997, pages 208-216, XP000199862 ISSN: 1066-2243 pag 210-211 Dynamic Domain Name System abstract	1-19